

TESTIMONY OF

O. Sami Saydjari

President, Professionals for Cyber Defense, a non-profit organization

Chief Executive Officer, Cyber Defense Agency, LLC

Former Director's Fellow, National Security Agency

**Former Program Manager of Information Assurance, Defense Advanced Research
Projects Agency**

Former Senior Executive Service, Defense Department

Founding Member, Cyber Conflict Studies Association

Department Editor, *IEEE Security & Privacy* Magazine

Before the

House Committee on Homeland Security

Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

**“Addressing the Nation’s Cyber Security Challenges: Reducing Vulnerabilities
Requires Strategic Investment and Immediate Action”**

April 25, 2007

Chairman Langevin, Ranking Member McCaul, and Members of the Subcommittee, it is a pleasure to have this opportunity to testify before you on an issue that is of utmost national urgency. I come to you as the leader of the Professionals for Cyber Defense, a non-profit group of recognized national cyber security leaders dedicated to advocating for the development of a sound cyber defense policy for the United States.

Summary. (1) The US is vulnerable to a strategically crippling cyber attack from nation-state-class adversaries. Cyber space primarily controls our real-world critical assets and is as legitimate a part of our territory as physical land, thus the government must *provide for the common defense* of this new territory. (2) A strategic multi-billion-dollar investment run by the country's best experts can mitigate this risk if we start now with \$500 million. (3) Congress can help today by supporting this funding level, advocating this initiative to Agency heads in a formal letter to motivate immediate discretionary investment, and leading the way by commissioning blue-ribbon panels and special investigative committees to help establish momentum.

Imagine the lights in this room suddenly go out, and we lose all power. We try to use our cell phones, but the lines of communication are dead. We try to access the Internet with our battery-powered laptops, but the Internet, too, is down. After a while, we venture out into the streets to investigate if this power outage is affecting more than just our building, and the power is indeed out as far as the eye can see. A passer-by tells us the banks are closed and the ATMs aren't working. The streets are jammed because the traffic lights are out, and people are trying to leave their workplaces en masse. Day turns to night, but the power hasn't returned. Radio and TV stations aren't broadcasting. The telephone and Internet still aren't working, so there's no way to check in with loved ones. After a long, restless night, morning comes, but we still don't have power or communication. People are beginning to panic, and local law enforcement can't restore order. As another day turns to night, looting starts, and the traffic jams get worse. Word begins to spread that the US has been attacked—not by a conventional weapon, but by a cyber weapon. As a result, our national power grid, telecommunications, and financial systems have been disrupted—worse yet, they won't be back in a few hours or days, but in months. The airports and train stations have closed. Food production has ceased. The water supply is rapidly deteriorating. Banks are closed so people's life savings are out of reach and worthless. The only things of value now are gasoline, food and water, and firewood traded on the black market. We've gone from being a superpower to a third-world nation practically overnight.

We saw what happened to the social fabric when Hurricane Katrina wiped out the infrastructure in a relatively small portion of our country: chaos ensued and the impact lasted a long time. What would be left after months of recovery from such devastation nationwide? Such strategic cyber attack scenarios are plausible and thus worthy of urgent attention. We are a nation *unprepared* to properly defend ourselves and recover from a strategic cyber attack.

My purpose today is to make a case for congressional action to support a major government initiative that could mitigate the risk of a devastating strategic cyber attack against the US. To understand the plausibility of such attacks without undertaking any action would be unconscionable. Even uncertainty by government leaders regarding such plausibility demands immediate action to remove the uncertainty and enable responsible policy decisions. The only rational approach to address a problem of this magnitude and scale is a concerted high-priority government program on the order of the Manhattan Project. Failure to embark on such a program now will have disastrous consequences to our national interests sooner rather than later.

I will now review the **case for action** our group made in a letter to President George W. Bush in 2002, highlight the true nature of the **national strategic threat** in a realistic cyber attack campaign called Dark Angel, outline the only reasonable **strategic countermeasure** in the form of an urgent, high-priority, multi-billion-dollar national program that we've dubbed the "Cyber Manhattan Project," point to some recent promising but woefully underfunded **cross-agency analysis and planning that affirms** both the grave situation and the need for a national program, and then I'll close with some recommendations on **moving forward**.

Background. In 1939, Albert Einstein felt duty-bound to warn President Franklin Roosevelt of a strategic threat to the country from nuclear weapons and the need for immediate action. In 2002, more than 50 leading cyber defense experts similarly felt compelled to warn President Bush of a strategic threat of a different kind, one to our critical information infrastructure. On 11 September 2001, terrorists used our air transport infrastructure against us and made a serious impact on both our economy and sense of security. Against a strong country such as the US, frontal attacks make little sense, but our vulnerability to infrastructure attacks makes such attacks increasingly likely.

The signers included a former Director of Central Intelligence, a former Director of the National Security Agency, a former Director of the Defense Advanced Research Projects Agency, and many of the nation's leading scientists and engineers. We warned President Bush that (a) the situation was grave, with nation-states such as China developing serious offensive capabilities, (b) a national initiative with priority, top talent, funding, and focus on par with the Manhattan Project was urgently needed to create cyber defense capabilities in close partnership with industry, (c) threading together components of national exercises, results from accidental information system failures, and actual cyber attacks, one could create devastating scenarios of strategic damage to the US, and (d) that the private-sector economy wouldn't solve the problem without government leadership because of a lack of incentive to do so. Since we signed the letter, little has changed with respect to the situation or the trend. It's time to move forward.

A subset of the signers formed a group called the Professionals for Cyber Defense (PCD) to engage in continuous advocacy. In summer 2002, the PCD panel reviewed the President's draft National Strategy to Secure Cyberspace. They found that the plan offered valuable advice to counter lower-grade threats but that it had a fundamental flaw in its unstated premise that there was no strategic national threat. In response, *we*

recommended that the government urgently initiate a scientific process to establish the scale, gravity, and validity of the national strategic threat of cyber war against our nation. We expected that such a process would validate the repeated warnings from the technical community in reports from the Defense Science Board, National Academy of Sciences, and the President's Commission.

But in our dialogue with the government, we learned of two barriers to aggressive action: (1) the perception that government investment would require "big government" private-sector interference, and (2) the case for national strategic vulnerability wasn't yet credible to senior leadership. In retrospect, on the first issue, we failed to realize that government leadership simply did not see cyber space as a territory on which we deeply depend and that must be protected and defended—rather, some people in leadership positions viewed it as an optional digital playground of bits and bytes for exchanging personal messages or looking at hobby information. But this isn't a matter of "big government" versus "small government"; it's a matter of our government stepping up to its constitutionally required duty to defend the US against threats beyond the capabilities and means of the private sector. We deeply understood the second issue, which is why we advocated for an urgent national-scale analysis of the vulnerability as the starting point for a program plan. In September 2002, the panel decided to sketch a case for action in the form of a realistic strategic cyber attack campaign against the US called "Dark Angel." This sketch was intended to be a starting point because it could demonstrate the problem's gravity.

The Threat: Dark Angel. What is the problem, and what is the solution? For the problem, we must ask if a strategic national vulnerability exists, what its scope is, and how bad "bad" can get. Without understanding the detailed nature of the problem, the efficacy of any proposed strategy is unknown. We must also ask why any proposed national strategy will solve the problem, and what happens if it doesn't. These seem like childishly simple questions, but the answers have been elusive. Indications are that national economic devastation is quite possible, and when we're in the middle of the disaster isn't the time to start thinking about how to respond. Preparing for cyber war will take in excess of three years and require infrastructure instrumentation for critical computer systems, experienced cadres of defenders who are well trained and exercised, control systems to execute strategic responses, effective architectures to mitigate risk, and a national program to create defensive capabilities. Thus, *understanding* the problem is an immediate need.

Planning. The small PCD planning team included a campaign planner, two experts in the financial sector, three in electrical power, and one in transportation. We assumed only unclassified critical infrastructure vulnerabilities. Our intent was to illustrate the damage a robust campaign that used multiple attack paths could cause and to create a plan with sufficient detail to convince experts in the domain. The plan took roughly 30 days to create. We assumed the adversary had three years of preparation, \$500 million, and 30 days to actually execute the attack. The attack campaign's goal was to destabilize the US and depress the economy with attacks on critical infrastructure, thus reducing our ability to project military power, depleting our will to fight, and creating panic and distrust in the government.

Our strategic campaign objectives included crippling rail transportation, rupturing oil and gas pipelines with improper control (for example, with cyber attacks similar to the one on the Soviet Trans-Siberian pipeline causing a three kiloton explosion, as described in “At the Abyss” by Thomas Reed), and creating widespread power outages by destroying hard-to-replace generators and power-line transformers with improper computer control commands. We also simulated attacks on financial services sectors, thus creating mass confusion in transaction settlement systems, flooded 911 systems with computer-controlled false alarms to create widespread panic, and disabled Internet service by performing denial-of-service attacks on the 13 main Domain Name Servers (as has already been partially done in actual cyber attacks).

In the simulated campaign, we spoofed attack attribution when possible to focus attention in the wrong direction; used lethal first strikes (for example, by hitting first responders and backups before hitting primary cyber targets); used a rolling attack barrage to interfere with recovery processes; delayed attacking instruments, such as the Internet, until that means was no longer needed in the campaign; bought cyber mercenaries and insiders as needed to gain capabilities and access; used non-cyber (physical) attacks on “tough” targets as needed; used psychological operations to create distrust in infrastructure and manipulate public opinion; and hampered the military by disrupting civilian re-supply chains.

Our simulated attacks were vetted with experts in each of the key critical infrastructure domains. The essence of the plan and its likely effects were verified. There was some uncertainty about the consequences of some attacks—even now—but this was due to a lack of knowledge among the entire community to fully assess such consequences. ***It would be hubris to think our adversaries don’t already have a plan in place that’s substantially better than our brief sketch or that their capabilities to execute such an attack aren’t improving.***

Follow-on. A proper national strategic threat assessment would parallel that of Dark Angel, and would involve top industry experts and business leaders, mix in military campaign planners, and mix in economists, policy makers, and others as needed. Sharing across industry should be encouraged and rewarded. From a management perspective, the assessment should carry presidential authority and priority. There should be three separate teams: one for planning and completing a concrete plan, one to execute the plan to the extent needed for demonstration purposes, and one to review the results for validity.

The assessment must start from the premise built into Dark Angel: that cyber warfare will be economic and social warfare. Diagnosis of the source of vulnerabilities must be included and reflect that the organization and design of our production systems will often be *more* important than cyber defense technology in determining the nature and extent of the destruction. What to defend and what kinds of damages to prevent are *not* self-evident without such an assessment.

For illustrative purposes, we estimate the resources needed for six critical infrastructure domains would take about \$70 million, 300 top-talent experts, and 9 calendar months.

The final report would be a definitive estimate of our true national strategic vulnerability to cyber attacks, a compelling case for action, and the basis of a prioritized program plan.

Countermeasure: Cyber Manhattan Project. As part of our dialogue with the government in 2002, we elaborated on the proper solution to the strategic vulnerability sketched out by our Dark Angel analysis. Cyber war defense requires orders of magnitude more government involvement and resources to avoid overwhelming national damages from strategic attacks. We recommended that the government (1) step up to a strong defense role against serious attacks, (2) focus on countering strategic attacks that have real-world effects, (3) develop a top-down architecture and engineered approach to the defined problem, (4) acknowledge that current technology is insufficient to defend against cyber war, and (5) divide the cost burden between the owner (to protect critical private cyber assets) and the government (to protect the integrity of the national commons).

As mentioned earlier, we chose the name “Cyber Manhattan Project” to reflect the urgency, priority, focus, top-talent, and funding levels needed. We acknowledge that aspects of the analogy are inapt, such as the fact that (1) there is no single, easily measurable artifact (such as a bomb), (2) a broad spectrum of talent and organizations must be involved, (3) much of the work must be conducted without classification constraint, and (4) once an initial capability is achieved, a continued investment will be needed to maintain our cyber defense’s effectiveness. We sketch the program below.

Vision. We must rapidly overcome our nation’s vulnerability to coordinated strategic cyber attacks from serious enemies.

Project Description. We need an aggressive, goal-directed, high-priority, national program to address the high-level threats that endanger the national well-being. To do this, we must engage the brightest scientists, business experts, and engineers, and provide them with adequate resources. To guide the program with strategic objectives, we need a top-down architecture that establishes concrete cyber defense capabilities on a specific timeline, including near-term capabilities within three years.

Capabilities. Some cyber defense capabilities to include are as follows: (1) capability to create system resiliency and quickly recover from inevitable partially successful attacks; (2) a national cyber Command, Control, Communication, and Computer Intelligence, Surveillance, and Reconnaissance (C4ISR) system to measure and control mechanisms at multiple echelon levels; (3) a national threat assessment capability to drive decisions at some “required” level; (4) cyber firebreak mechanisms and architectures to slow down attacks and reduce potential damage; (5) capability to gather intelligence and inject uncertainty through strategic deception; (6) capability to model and simulate the enemy, thereby honing our defenses before incurring damaging strategic cyber attacks; and (7)

capability to identify and understand available and acceptable responses from technical, strategic, legal, economic, and political perspectives.

Urgency. Major potential adversaries are actively pursuing cyber war capabilities, which indicates the increasing probability of future cyber campaigns. Moreover, (a) current cyber defenses and best practices are ineffective, (b) active measures to shut down our adversaries' abilities to attack through physical access will drive them to cyber space, and (c) we face potentially greater vulnerability and lethality from combined cyber and physical attacks. Finally, ***developing a defense to this threat is a multiyear effort, so we can't wait until we find ourselves suffering in the midst of our first major strategic attack campaign.***

Priority. A major initiative on the order of the Cyber Manhattan Project is *the* right path to address our current situation. The offensive threat is growing, so defense must be fielded at a faster rate. A top-down approach with a driving architect can address the problem and achieve the requisite objectives, but bottom-up efforts, even if coordinated, leave gaps because there's no ownership of key parts of the problem. Cyber defense mechanisms must integrate into a coordinated system, and cyber defense operations must comprise a fully integrated defensive force. For success, the creation of national cyber defense capabilities must be a national funding priority. Can you imagine the original Manhattan Project succeeding without such a focus?

Feasibility. Not only is the creation of national cyber defense capabilities critically urgent and important, it's also feasible. (1) Technically, many effective defensive technologies exist but are in research stages and must be transitioned to operational use; some already have limited field testing, and others already exist to address broad classes of novel attacks. Moreover, the required computational resources for intensive activities such as correlation of attack and modeling/simulating attack strategies and tactics are available today. Ongoing research sponsored by the likes of NSA, NSF, DOD, DNI, DHS, and others is beginning to address additional hard science problems. (2) Economically, we can make a national business case for investing in a program intended to avoid the expected financial losses from strategic cyber attacks and ensure the proper public-private sharing of the burden. (3) Operationally, we can manage the complex infrastructure through judicious use of automation with a capable cadre of defenders. Through a combination of reasonable fire-code-like cyber security standards, improved operational guidance, and trained/experienced personnel, we would also be able to contain mission and cost impacts in the short term while we develop new capabilities. (4) Politically, public awareness of the threat is likely to make needed investments and standards acceptable. Industry is increasingly aware that nation-state-level attacks are a concern beyond their current ability to handle, yet they threaten business continuity. With proper financial incentives and partnering for workable solutions, industry is likely to openly embrace government involvement and protection. (5) Finally, from a schedule perspective, a phased rollout of capabilities based on threat prioritization and available technologies is also feasible. Success is certainly not assured, but the alternative is to begin radically reducing our dependency on computing systems, which would seriously degrade our national competitiveness and suppress economic growth. The cyber

vulnerabilities in our infrastructures have become deeply embedded and widespread through the economic forces that drive individual companies to reduce costs by adopting the most widely available and interoperable technologies. It won't be easy to develop a cyber infrastructure that can resist strategic attacks—it will require short-term actions as well as a long-term plan and a willingness to keep that plan in focus over a number of years.

Plan of Action. We recommend assigning a government lead responsible for creating a plan. The PCD offers to work with this lead and recommends a three-month deadline for developing a “blueprint” to launch the project, including technical and program management aspects. We also recommend jumpstarting a multiyear program now with as much seed funding as possible.

The PCD hasn't worked out a full recommendation for how a Cyber Manhattan Project, which would inherently involve multiple agencies, ought to be organized and managed. A few points of consensus, though, appear to be emerging. (1) Distributing a surge of funding to the myriad bureaucracies that currently fund cyber defense won't work in the long run. Each bureaucracy pulls in a different direction, making focused investment nearly impossible, although a jumpstart in 2007/2008 might have to start this way out of sheer practicality. (2) Centralizing funding and government-wide responsibility in one existing department or agency with its own mission will likely cause the funding to be spent by that bureaucracy's priorities, to the detriment of national interest. (3) Creating a whole new department or agency might fall into the too-hard-to-do pile, given the tremendous distractions and delays involved (as we've seen with the startup of the Department of Homeland Security).

Eventually, what we need is a centralized, light-weight, high-level controlling body to create a focused effort on national cyber defense capabilities. One thought has been to create a special projects office accountable to and operating with the authority of the White House, with an elite staff of 200 people, at least half of the overall program budget, and some purview over the spending of the other half distributed and executed by existing organizations.

Recent Developments. Recent activities tend to echo and affirm the PCD's earlier findings. In November 2006, in response to concerns of inherent computer system vulnerabilities and escalating threats, more than 60 experts in system security, processor design, operating systems, programming languages, networking, and applications from diverse backgrounds in academia, government, and industry met to consider past, current, and possible future approaches to building systems with improved security. Findings from this Safe Computing Workshop included the following: (1) attackers rule, disasters are likely; (2) short-term measures are essential but insufficient; (2) market forces won't change the balance; (3) usability and manageability must be part of the solution; (4) new technology can catalyze major changes; and (5) only a national initiative will make a real difference.

The workshop participants also concluded that the timing of such an investment is particularly good now because (1) significant advances in technology have dramatically increased hardware processing, memory, and communication capacity; (2) there's a growing understanding of the problem among the public and government leadership as everyday cyber attacks like spam, phishing, and identity theft become increasingly painful; (3) industry's interest in cyber security continues to grow as the community becomes more adept at making a business case for improvements; (4) escalating attacks and damages are increasing across the globe; (5) major software vendors are willing to delay the release of their products for more than a year to forestall security embarrassments; and (6) without a major change in direction, adversaries will be able to exploit current weaknesses in US cyber security and could deal a critical blow to our country's major industrial sectors, such as banking, energy, and telecommunications. ***The workshop participants found a compelling and urgent need to dramatically reduce the vulnerability of the national information infrastructure to attack, and that major, strategic investments could significantly reduce our vulnerability over a five-year period.***

Closing Remarks.

Smoking Gun. Some of you might think, what's the rush? Where's the smoking gun—the indication of a major assault on US cyber infrastructure? Surely, it's coming, and it's no doubt already in its planning stages. We suggest three reasons for why this is so. First, strategic long-term damage requires substantial planning and very well-timed execution. Creating the capabilities and placing the required assets (such as insiders) takes time, certainly years. Second, when such a cyber attack weapon is created, it's in some sense a one-time-use strategic option. One wouldn't use it lightly, nor would one want to tip one's hand about it until it's really needed: such weapons may well be deployed already, and we wouldn't know it (perhaps a sleeper cell of insiders and/or malicious software embedded in our critical infrastructure). Finally, our current cyber infrastructure offers a wealth of highly valuable knowledge (such as advanced research results). As adversaries conduct espionage, they're also mapping our cyber space and gaining great experimental and training experience that will enable future strategic attacks. It's in the interests of our adversaries to preserve their upper hand for as long as possible and keep tapping into these important attributes. Moreover, such nation-state network exploitations are becoming increasingly obvious to the point that the mainstream press regularly covers them.

Secrecy. We don't advocate that a Cyber Manhattan Project be shrouded in secrecy: doing so would be unnecessary and deleterious to the program goals. The nation's best minds must work on this difficult problem, and many of them are to be found outside government in academia and industry. Excluding those minds by making the program secret would only decrease our chances of success. Obviously, it makes some sense to maintain the element of surprise about the details of some of our planned defenses, but these should be carefully thought out and very limited in scope. A design that counts on its own secrecy to succeed isn't a robust design at all: we all know how fleeting secrets can be.

Stakes. But what if we don't do this? Ladies and gentleman, based on the vetted Dark Angel scenarios, we could compromise our country as we know it if we make a misstep today. Inaction isn't an option for any of us who now know these stakes and are entrusted by the people to *provide for the common defense* and protect the future of our great country. Thank you.

Exhibit 1: Full Letter to President as Image to include actual signatures

27 February 2002

George W. Bush
President of the United States
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Mr. President,

Our nation is at grave risk of a cyber attack that could devastate the national psyche and economy more broadly than did the September 11th attack. We, as concerned scientists and leaders, seek your help and offer ours. The critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster. We urge you to act immediately by forming a Cyber-Warfare Defense Project modeled in the style of the Manhattan Project.

Consider the following scenario. A terrorist organization announces one morning that they will shut down the Pacific Northwest electrical power grid for six hours starting at 4:00 PM; they then do so. The same group then announces that they will disable the primary telecommunication trunk circuits between the U.S. East and West Coasts for a half day; they then do so, despite our efforts to defend against them. Then, they threaten to bring down the air traffic control system supporting New York City, grounding all traffic and diverting inbound traffic; they then do so. Other threats follow, and are successfully executed, demonstrating the adversary's capability to attack our critical infrastructure. Finally, they threaten to cripple e-commerce and credit card service for a week by using several hundred thousand stolen identities in millions of fraudulent transactions. Their list of demands is then posted in the New York Times, threatening further actions if their demands are not met. Imagine the ensuing public panic and chaos. If this scenario were to unfold, Americans everywhere would feel that our national sovereignty had been compromised; we would wonder how, as a nation, we could have let this happen.

Mr. President, what makes this scenario both interesting and alarming is that all of the aforementioned events *have* already happened, albeit not concurrently nor all by malicious intent. They occurred as isolated events, spread out over time; some during various technical failures, some during simple (government-sponsored) exercises, and some during real-world cyber attacks. All of them, however, could be effected through remote cyber attack by any adversary who so chooses, whether individual or state-sponsored. The resources required are modest—far less than the cost of one army tank. All that is required is a small group of competent computer scientists, a few inexpensive PCs, and Internet access. Even the smallest nation-states and terrorist organizations can easily muster such capabilities, let alone better-organized groups such as Al Qaeda.

Many nations, including Iran and China, for example, have already developed cyber-offense capabilities that threaten our economy and the economies of our allies.

There is no doubt that such a serious national vulnerability is a real and present danger. This has been affirmed by a number of distinguished bodies, including the President's Commission on Critical Infrastructure Protection (1997), the National Academy of Sciences (Computers at Risk, 1990; Trust in Cyberspace, 1999), and the U.S. Defense Science Board on Information Warfare Defense (1996, 2000).

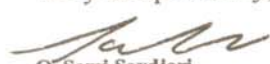
The consequence of successfully exploiting these vulnerabilities would be significant damage to the U.S. economy, degraded public trust with concomitant long-term retardation of economic growth, degradation in quality of life, and a severe erosion of the public's confidence that the government can adequately protect their security. We have seen the amplification effects, on our economy and on public apprehension, from a single event such as the World Trade Center and Pentagon attacks. Aggregate damages resulting from amateur cyber attacks (e.g., 1998 Internet Worm, Melissa Virus, I-LOVE-YOU virus, Code Red Virus and the Nimda virus) are estimated to have been \$12 billion for the year 2001 alone. Extrapolating from this, a professionally-executed, coordinated cyber attack on our national critical infrastructure could easily result in a 100-fold amplification— 10-fold from being professionally-executed and another 10-fold from indirect e-commerce suppression effects. In terms of a dollar value, this could amount to several hundred billion dollars in damage to the U.S. economy. Moreover, some community experts and reports (such as those cited above) estimate a high probability of a serious attack on U.S. critical infrastructure within the next few years.

The goal of our proposed Manhattan-style undertaking would be to create a national-scale cyber-defense policy and capability to prevent, detect, and respond to cyber threats to our critical infrastructure. We mean Manhattan-style in several senses: national priority, inclusion of top scientists, focus, scope, investment, and urgency with which a national capability must be developed. To prevent attacks, we need a coordinated effort to work with our critical-infrastructure providers in defending their most critical information systems. To detect attacks, we need to permeate our critical networks with a broad sensor grid imbued with the capability to detect large-scale attacks by correlating and fusing seemingly unrelated events that are, in fact, part of a coordinated attack. To respond to attacks, we need to devise strategies and tactics to pre-plan effective actions in the face of major cyber-attack scenarios; we need to augment our national infrastructure with mechanisms that support the defined strategies and tactics when attacks are detected and verified. We believe that all this can be done with a close partnership between the public and private sectors while maintaining sensitivity to public concerns about privacy and fairness, consistent with American values and laws. The result should be a resilient critical infrastructure that is resistant to cyber attack, plus next-generation technology which enables our critical infrastructure to be more easily secured. Given private-sector economic realities, our nation's economy and well-being will continue to rely on the existing vulnerable infrastructure for the indefinite future, unless strong government investment leads the way.

The proposed Manhattan-style cyber-defense project will cost a fraction of the expense we will incur from a single major cyber attack. We estimate the project would require an investment of \$500 million per year initially, and could reach the billion dollar level in the out-years. The project would run over the course of five years to create a national-scale initial operating capability no later than year three, and more advanced defensive and offensive capabilities by year five. We recommend that you appoint a small board of top computer scientists and engineers to work out the details of a plan, and set the plan in motion within ninety days. The plan should include an appropriate balance between engineering and focused research to support the national capability and the policy, laws, and procedures that would be needed to deploy and support the cyber-defense technology.

The clock is ticking. We look to you, as America's leader, to act on behalf of the nation. Your conscientious and effective defense of our physical homeland should extend into the increasingly vital frontier of U.S. cyberspace. We anticipate that the nation will fully endorse and even expect this forward-thinking and courageous action in the face of such a major threat to national security. We stand ready to help in any way we can in taking this important next step to defend our country.

Very Respectfully,



O. Sami Saydjari
Founder Cyber Defense Research Center
Former Information Assurance Program
Manager, DARPA
Former Fellow, National Security Agency



Salvatore J. Stolfo
Professor of Computer Science
Columbia University



Roy A. Maxion, Ph.D.
Director, Dependable Systems Laboratory
Computer Science Department
Carnegie Mellon University



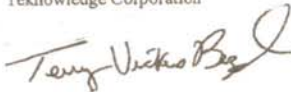
Dr. Robert Balzer
Chief Technology Officer
Teknowledge Corporation



Dr. Curtis R. Carlson
Chief Executive Officer
SRI International



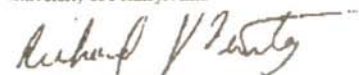
David J. Farber
Moore Professor of Telecommunications
and Professor of Business and Public
Policy
University of Pennsylvania



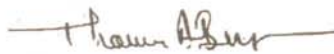
Terry C. Vickers Benzel
Vice President of Advanced Security
Research
Network Associates, Inc.



George Cybenko
Dorothy and Walter Gramm Professor
Thayer School of Engineering
Dartmouth College



Richard J. Feiertag
Manager of Strategic Planning
NAI Labs, Security Research Division
Network Associates, Inc.



Thomas A. Berson, Ph.D.
Principal Scientist, Palo Alto Research
Center
Past-President, International Association
for Cryptologic Research
Past-Chair, IEEE Technical Committee on
Security and Privacy



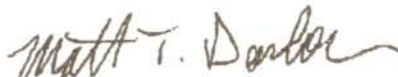
John C. Davis
Director of Information Security
Mitretek Systems, Inc.
Former Commissioner on PCCIP
Former Director of NCSC/NSA



Edward A. Feigenbaum
Kumagai Professor of Computer Science
Emeritus
Stanford University, and
Chief Scientist, United States Air Force
(1994-97)



Bob Blakely
Chief Scientist, Security and Privacy
IBM Tivoli Software



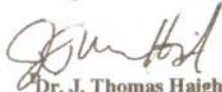
Matt Donlon
Former Director, Security and Intelligence
Office
Defense Advanced Research Projects
Agency



Dr. Tiffany M. Frazier
Director, Advanced Computing
Alphatech, Inc.



Seymour E. Goodman
Professor of International Affairs and
Computing
Co-Director, Georgia Tech Information
Security Center
Georgia Institute of Technology



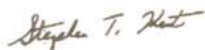
Dr. J. Thomas Haigh
Chief Technology Officer
Secure Computing Corporation



Walter L. Heimerdinger, PhD



Patrick M. Hughes
Lieutenant General, U.S. Army, Retired
President, PMH Enterprises LLC
Former Director, Defense Intelligence
Agency
Former Director of Intelligence (J-2),
Joint Chiefs of Staff



Stephen T. Kent
Chief Scientist - Information Security
BBN Technologies - A Verizon Company
(member of "Computers at Risk" & "Trust
in Cyber Space" NRC committees)



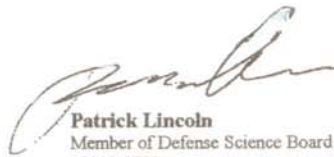
Angelos D. Keromytis
Assistant Professor,
Computer Science Dept.
Columbia University



Dr. Marvin J. Langston
Deputy Chief Information Officer,
Department of Defense, 1998-2001
Director Information Systems Office,
Defense Advanced Research Projects
Agency, 1997-98
Chief Information Officer, Department of
Navy, 1996-1997



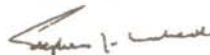
Karl N. Levitt
Professor of Computer Science
Director of the UC Davis Security
Laboratory
Department of Computer Science
University of California, Davis



Patrick Lincoln
Member of Defense Science Board Panels
2000-2001
Director, Computer Science Laboratory
SRI International



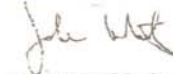
John H. Lowry
Division Engineer
Technical Director for Information
Security
BBN Technologies/Verizon



Stephen J. Lukasik
Consultant, Science Applications
International Corporation
Former Director, Department of Defense
Advanced Research Projects Agency
Former Chief Scientist, Federal
Communications Commission



David Luckham
Research Professor of Electrical
Engineering
Stanford University



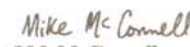
Dr. Joseph Markowitz



Robert T. Marsh
General, USAF (Retired)
Former Chairman, President's
Commission on Critical Infrastructure
Protection



Terry Mayfield
Institute for Defense Analyses



J.M. McConnell
Former Director, National Security
Agency



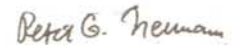
John McHugh, PhD
Carnegie Mellon University



Roderick A. Moore
Systems Engineer
Former National Security Council Staff
Pres. Reagan and Pres. Bush
Administrations



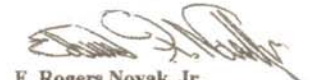
Dr. Charles L. Moorefield
Board Chairman,
Alphatech, Inc.



Peter G. Neumann
Computer Science Lab
SRI International



Dr. Clifford Neuman
Sr. Research Scientist and Associate
Division
Director - Computer Networks Division
Information Sciences Institute
University of Southern California



E. Rogers Novak, Jr.
Managing Member
Novak Biddle Venture Partners



Allen E. Ott
Orincon Information Assurance
President



Dr. Michael Paige
Former Director, Xerox PARC



Dr. Vern Paxson
Senior Scientist, International Computer
Science Institute
Staff Scientist, Lawrence Berkeley
National Laboratories



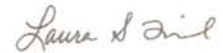
Phillip A. Porras,
Program Director
System Design Laboratory
SRI International



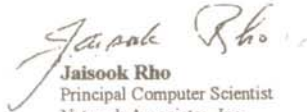
Marcus Ranum
Chief Technology Officer
NFR Security, Inc.



Fred B. Schneider
Professor of Computer Science and
Director of Cornell/AFRL Information
Assurance Institute



Laura S. Tinnel
Deputy Program Manager and Research
Scientist
Information & Systems Assurance Group
Teknowledge Corporation



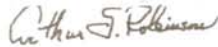
Jaisook Rho
Principal Computer Scientist
Network Associates, Inc.



Gregg Schudel
Formerly, Senior Engineer and Manager
of Experimentation, DARPA
Information Assurance Program



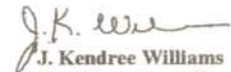
J. Douglas Tygar
Professor of Computer Science and
Information Management
University of California, Berkeley



Dr. Arthur S. Robinson
President, System/Technology
Development Corporation
Formerly Technical Director of RCA
R&D for U.S.N. Aegis Weapons
Systems



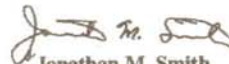
Larry J. Schumann
President, EnterpriseTec, Inc.
Member of the President's National
Security Telecommunications Advisory
Committee (1996-2000)



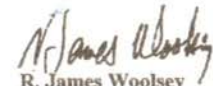
J. Kendree Williams
Chief Technology Officer
Zel Technologies, LLC
CDR, USN (Ret)



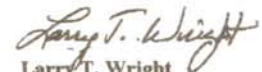
S. Shankar Sastry
Professor and Chair, Department of
Electrical Engineering and Computer
Sciences
Formerly, Director, Information
Technology Office, DARPA, US DoD



Jonathan M. Smith
Professor
Computer and Information Science
Department
University of Pennsylvania



R. James Woolsey
Director of Central Intelligence, 1993-95



Larry T. Wright
Chairman, Defense Science Board
Task Force on Defensive Information
Operations
2000-2001

